

REMARKS

By this Amendment, claims 1-2, 6, 9-10, 13-14, 18-19 and 21-22 are amended. Claims 3-5, 7-8, 11-12, 15-17 and 20 remain in the application. Thus, claims 1-22 are active in the application. Reexamination and reconsideration of the application are respectfully requested.

On page 4 of the Office Action, claims 1-22 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicants regard as the invention. In particular, the Examiner asserted that claims 1-22 are incomplete for omitting essential structural cooperative relationships of elements because it is unclear how the encryption processing and the authentication processing can occur both in parallel and sequentially.

Claims 1 and 18 have each been amended to clarify the cooperative relationships of the elements and more clearly define how the encryption processing and the authentication processing are performed in parallel.

In particular, claim 1 has been amended to recite that “when the inputted packet is a packet which requires both encryption processing and authentication processing, the encryption processing of the data block having the B1 bit length by the at least one encryption processing unit and the authentication processing of the data block having the B2 bit length by the at least one authentication processing unit are performed in parallel.” Further, claim 1 has been amended to recite that the data block accumulation unit, which is placed between the encryption processing unit and the authentication processing unit, is “operable to accumulate the data blocks each having the B1 bit length on which the encryption processing has been performed by the at least one encryption processing unit, and, when the number of accumulated encrypted blocks each having the B1 bit length reaches n, output the data block having the B2 bit length made up of the n data blocks each having the B1 bit length, to the at least one authentication processing unit.”

In addition, the wherein clauses added to claim 1 further define how the present invention performs the encryption processing and the authentication processing both in parallel and sequentially.

Accordingly, claim 1 provides that the encryption processing and the authentication processing are performed in parallel as pipeline processing, although the

bit length of the data block to be encrypted is different from the bit length of the data block to be authenticated. The method of claim 18 was amended similar to claim 1.

In view of the above amendments to claims 1 and 18, the Applicants respectfully submit that claims 1 and 18 clearly and particularly define how the encryption processing and the authentication processing can occur both in parallel and sequentially. Therefore, the Applicants respectfully request withdrawal of the rejection of claims 1-22 under 35 U.S.C. § 112, second paragraph.

On page 8 of the Office Action, the Examiner reiterated the rejection of claims 1-2, 5-6, 9, 13 and 17-20 under 35 U.S.C. § 102(e) as being anticipated by Mathews (U.S. Patent Application Publication No. 2002/0078342). This rejection is respectfully traversed for the following reasons.

The present invention provides a security communication packet processing apparatus and method that, relative to conventional systems, makes it possible to speed up processing, reduce delay of the processing, increase throughput for a packet which requires authentication processing after encryption processing (although the authentication value does not need to be encrypted).

To achieve these features, the security communication packet processing apparatus of claim 1 recites that when the inputted packet is a packet which requires both encryption processing and authentication processing, the encryption processing of the data block having the B1 bit length by the at least one encryption processing unit and the authentication processing of the data block having the B2 bit length by the at least one authentication processing unit are performed in parallel.

Further, as described above, the data block accumulation unit, which is placed between the encryption processing unit and the authentication processing unit, accumulates the data blocks each having the B1 bit length on which the encryption processing has been performed by the at least one encryption processing unit, and, when the number of accumulated encrypted blocks each having the B1 bit length reaches n, output the data block having the B2 bit length made up of the n data blocks each having the B1 bit length, to the at least one authentication processing unit. The method of claim 18 recites these features.

Therefore, the encryption processing and the authentication processing are

performed in parallel as pipeline processing, although the bit length of the data block to be encrypted is different from the bit length of the data block to be authenticated. This feature of the present achieves a reduction in the buffer size of the data block accumulation unit, as well as high-speed encryption processing and authentication processing.

In contrast to the present invention, Mathews does not disclose such parallel processing of encryption and authentication on data blocks of different bit lengths. Instead, Mathews performs parallel processing of a packet of plain text which requires encryption processing and authentication processing, where the authentication value needs to be encrypted.

In particular, Mathews discloses that the chip architecture includes an authentication component 302 and an encryption (or decryption) component 352. The authentication component 302 includes an authentication alignment block 304 which removes non-valid bytes of a packet and packs and aligns data to be input into an authentication FIFO buffer 306 (see paragraph [0027]). Once 512 bits or a complete packet worth of data padded to a multiple of 512 bits have been loaded into the authentication FIFO buffer 306, Mathews discloses that the authentication value is then fed back into the encryption component 352. Specifically, the encryption alignment block 354 receives data for cryptography processing from a front end source 301 and the feedback of the authentication value outputted from the authentication engine 308 (see arrow 309 of Figure 3 and paragraphs [0028]-[0031]).

Furthermore, for processing a packet or stream of data that requires both encryption processing and authentication processing, Mathews discloses that the authentication value must then be encrypted by the encryption alignment block 354. In addition, Mathews includes respective buffers in the stages prior to the authentication processing (FIFO 306) and the encryption processing (FIFO 356). In particular, Mathews requires a buffer of an authentication value size (512 bits) or larger (that is, larger than the encryption block size) in the stage prior to the encryption processing.

Accordingly, in view of the above, Mathews clearly does not disclose the parallel processing of encryption and authentication on data blocks of different bit lengths, as recited in claims 1 and 18.

Furthermore, claim 1 recites a packet construction unit (corresponding to the reconstructing operation in claim 18) operable to (i) receive, from the at least one encryption processing unit, and accumulate, one by one, the encrypted data blocks corresponding to the data blocks obtained by dividing the inputted packet, (ii) receive the authentication value from the at least one authentication processing unit, and (iii) reconstruct the processed packet by using a set of the accumulated encrypted data blocks and the authentication value.

This feature of the present invention achieves reconstruction of a processed packet corresponding to an inputted packet by performing encryption processing and authentication processing on the inputted packet, and therefore realizes a useful and novel device and method which convert an ordinary packet into a packet that is suitable for secure communication.

The Applicants respectfully submit that Mathews clearly does not disclose or suggest the packet construction unit or operation, namely, a packet construction unit and operation which reconstruct a processed packet by using a set of accumulated encrypted data blocks and an authentication value.

For at least the foregoing reasons, claims 1 and 18 are clearly not anticipated by Mathews since Mathews fails to disclose or suggest each and every limitation of claims 1 and 18.

On page 16 of the Office Action, the Examiner reiterated the rejection of claims 3-4, 7-8, 10-12 and 14-16 under 35 U.S.C. § 103(a) as being unpatentable over Matthews in view of Videcrantz et al. (U.S. 6,275, 588).

As demonstrated above, Mathews clearly fails to disclose or suggest each and every limitation of claims 1 and 18. Specifically, Mathews fails to disclose or suggest the parallel processing of encryption and authentication on data blocks of different data blocks, and the reconstruction of a processed packet by using a set of accumulated encrypted data blocks and an authentication value, as recited in claims 1 and 18.

However, Videcrantz et al. fails to cure the deficiencies of Mathews for failing to disclose or suggest each and every limitation of claims 1 and 18.

Therefore, no obvious combination of Mathews and Videcrantz et al. would result in the inventions of claims 1 and 18 or any claims depending therefrom since Mathews

and Videcrantz et al., either individually or in combination, fail to disclose or suggest each and every limitation of claims 1 and 18.

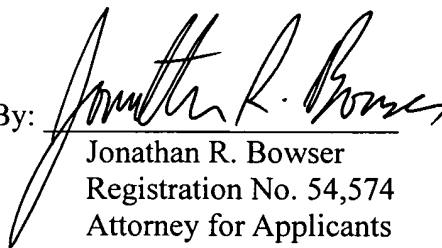
Furthermore, it is submitted that the clear distinctions discussed above are such that a person having ordinary skill in the art at the time the invention was made would not have been motivated to modify Mathews and Videcrantz et al. in such a manner as to result in, or otherwise render obvious, the present invention as recited in claims 1 and 18. Therefore, it is submitted that the claims 1 and 18, as well as claims 2-17 and 19-22 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

Yuusaku OHTA et al.

By: 
Jonathan R. Bowser
Registration No. 54,574
Attorney for Applicants

JRB/nrj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 15, 2006